UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/079,747	02/19/2002	Shu-Fan Liu	67,200-618	9116

7590 03/22/2005

TUNG & ASSOCIATES
Suite 120
838 W. Long Lake Road
Bloomfield Hills, MI 48302

EXAMINER	
TAYLOR, NICHOLAS R	
ART UNIT	**PAPER NUMBER**
2141	

DATE MAILED: 03/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/079,747	LIU, SHU-FAN	
	Examiner	Art Unit	
	Nicholas R Taylor	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 have been examined and are rejected.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, claim 17 repeats the limitation defining n equal to three seconds, which was previously defined in claim 15.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US Patent 6,178,511) and Moran (US Patent 6,826,697.)

6. As per claim 1, Cohen teaches a single sign-on computer system (Cohen, column 4, lines 35-60) comprising:

(a) a client device capable of communicating with a server network; (b) a server network, the server network comprising: (Cohen, column 3, lines 62-67)

an account collaboration agent server, the account collaboration agent server in communication with the client device; (Cohen, column 4, line 61 to column 5, line 6)

at least one web server for accessing at least one associated target web-based application, and wherein the at least one web server is in communication with the account collaboration agent server; (Cohen, column 4, lines 22-35, and figure 3)

at least one database server associated with the at least one web server, the at least one database server in communication with the at least one web-server and in further communication with the account collaboration agent server; and (c) means for securely defining a user profile, the user profile capable of being retrieved by the account collaboration agent server (Cohen, column 5, lines 7-30.)

However, Cohen does not specifically teach the at least one web server having an associated time clock. Moran teaches managing a synchronized system clock (Moran, column 37, lines 18-61.) It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to have combined Cohen and Moran to provide the clock functionality of Moran in the system of Cohen, because doing so would allow improved detection of network intrusions (Moran, column 3, lines 18-20.)

7. As per claim 2, Cohen-Moran teaches the system further wherein the account collaboration agent server further comprises memory means for securely storing the user profile there within (Cohen, column 5, lines 7-30.)

8. Claims 3-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US Patent 6,178,511) and Moran (US Patent 6,826,697), further in view of Belapurkar et al. (US PGPub 2003/0065956.)

9. As per claim 3, Cohen-Moran teaches the system further wherein the account collaboration agent server further comprises:

(a) means for securely retrieving the user profile from the memory means, wherein the user profile comprises a user identification and an associated user password; (Cohen, column 5, lines 7-30)

(c) means for timing an amount of time a user accesses the single sign on system, the means for timing comprises a clock counter, and wherein the clock counter initializes and begins counting the time once the user profile is retrieved from the user profile memory means, and stops counting once a user having the associated user profile logs off of the single sign on system; (Moran, column 21, lines 6-20)

(d) means for synchronizing the clock counter with the at least one web server time clock; (Moran, column 37, lines 41-61)

(f) means for defining a database schema, wherein the schema allows secure communications between the account collaboration agent server, the at least one web server, and the associated at least one server database (Cohen, column 5, lines 7-30.)

However, Cohen-Moran fails to teach:

(b) means for building a secure connection string between the client device and the server network; and

(e) at least one session variable index register for indexing a user's session variables, the session variables comprise an authenticated and authorized user identification and a timestamp associated with the user identification, the timestamp is an indicated time value extracted from the clock counter when an authenticated and authorized user requests access to the at least one web server target application.

Belapurkar teaches a means of building a secure connection string (Belapurkar, paragraph 0029) using a timestamp associated user identification during an access request (Belapurkar, paragraph 0028), in a method for secure data transmission in a single sign-on (SSO) system (Belapurkar, paragraph 0042.) It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to have combined Cohen-Moran and Belapurkar to provide the secure string and timestamp of Belapurkar in the system of Cohen-Moran, because doing so would enable the secure transmission of data in a single sign-on system (Belapurkar, paragraph 0006.)

10. As per claim 4, Cohen-Moran-Belapurkar teaches the system further wherein the means for defining a database schema further comprises an account collaboration

program for executing control over the session variables to securely communicate the session variables from the account collaboration agent server to the at least one web-based server when a user requests access to the at least one web-based server (Cohen, column 5, lines 7-30.)

11. As per claim 5, Cohen-Moran-Belapurkar teaches the system further wherein the an account collaboration program is replicated in the at least one web server (Belapurkar, paragraph 0044.)

12. As per claim 6, Cohen-Moran-Belapurkar teaches the system further wherein the at least one database has a user identification index register stored within for indexing the user identification (Cohen, column 5, lines 7-30.)

13. As per claim 7, Cohen teaches a single sign-on computer system (Cohen, column 4, lines 35-60) comprising:

(a) a client device capable of communicating with a server network; (b) a server network, the server network comprising: (Cohen, column 3, lines 62-67)

at least a first web server for accessing at least one first associated target web-based application, the at least first web server having an associated first database server in communication with the at least one first web server, and at least a second web server for accessing at least one second associated target web-based application, the at least one second web server having an associated second database server in

communication with the at least one second web server, and, (Cohen, column 4, lines 22-35, and figure 3)

an account collaboration agent server in communication with the client device, the first web server, and the second web server, the account collaboration agent server comprises: (Cohen, column 4, line 61 to column 5, line 6)

means for securely retrieving a user profile, wherein the user profile comprises a user identification and an associated user password, (Cohen, column 4, line 61 to column 5, line 6.)

means for defining a database schema, wherein the schema allows secure communications between the account collaboration agent server, the at least two web servers, and their associated at least two server databases; and (c) means for defining a user profile, the user profile capable of being retrieved by the account collaboration agent server (Cohen, column 5, lines 7-30.)

However, Cohen fails to teach for the first and second servers, wherein the at least one web server has an associated time clock, and means for synchronizing the clock counter with the at least two web servers time clocks; and (Moran, column 37, lines 41-61) and

means for timing an amount of time a user accesses the single sign on system, the means for timing comprises a clock counter, and wherein the clock counter initializes and begins counting the time once the user profile is accessed, and stops counting once a user having the associated user profile logs off of the single sign on system.

Moran teaches managing a clock (Moran, column 37, lines 18-61) that is also synchronized (Moran, column 37, lines 41-61), wherein timing the user sessions is achieved (Moran, column 21, lines 6-20.) It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to have combined Cohen and Moran to provide the clock functionality of Moran in the system of Cohen, because doing so would allow improved detection of network intrusions (Moran, column 3, lines 18-20.)

However, Cohen-Moran fails to teach means for building a secure connection string between the client device and the server network, and

at least one session variable index register for indexing a user's session variables, the session variables comprise an authenticated and authorized user identification and an initial timestamp associated with the user identification, the initial timestamp is an indicated time value extracted from the clock counter when an authenticated and authorized user requests access to the at least one web server target application.

Belapurkar teaches a means of building a secure connection string (Belapurkar, paragraph 0029) using a timestamp associated user identification during an access request (Belapurkar, paragraph 0028), in a method for secure data transmission in a single sign-on (SSO) system. It would have furthermore been obvious to one of ordinary skill in the art, at the time the invention was made, to have combined Cohen-Moran and Belapurkar to provide the secure string and timestamp of Belapurkar in the system of Cohen-Moran, because doing so would enable the secure transmission of data in a single sign-on system (Belapurkar, paragraph 0006.)

14. As per claim 8, Cohen-Moran-Belapurkar teaches the system further wherein the account collaboration agent server further comprises memory means for securely storing the user profile there within (Cohen, column 5, lines 7-30.)

15. As per claim 9, Cohen-Moran-Belapurkar teaches the system further wherein the means for defining a database schema further comprises an account collaboration program for executing control over the session variables to securely communicate the session variables from the account collaboration agent server to the at least one web-based server when a user requests access to the at least one web-based server (Cohen, column 5, lines 7-30.)

16. As per claim 10, Cohen-Moran-Belapurkar teaches the system further wherein the an account collaboration program is replicated in the at least two web servers (Belapurkar, paragraph 0044.)

17. As per claim 11, Cohen-Moran-Belapurkar teaches the system further wherein the at least first associated database has a first web-server session variable index register for indexing a users first web-server session variables, the first session variables comprise an authenticated and authorized user identification (Cohen, column 5, lines 7-30) and an associated first web-server timestamp, the associated first web-server timestamp is an indicated first time variable extracted from the first web server

time clock when an authenticated and authorized user requests access to the at least second web server target application (Belapurkar, paragraph 0028.)

18. As per claim 12, Cohen-Moran-Belapurkar teaches the system further wherein the at least second associated database has a second web-server session variable index register for indexing a users second web-server session variables, (Cohen, column 5, lines 7-30) the second session variables comprise an authenticated and authorized user identification and an associated second web-server timestamp, the associated second web-server timestamp is an indicated second time variable extracted from the second web server time clock when an authenticated and authorized user requests access to the at least first web server target application (Belapurkar, paragraph 0028.)

19. As per claim 13, Cohen-Moran-Belapurkar teaches the system further comprising the steps of

logging a user into the single sign on system; (Cohen, column 4, lines 35-60)

building a secure connection string between the account collaboration agent server and the client device; (Belapurkar, paragraph 0029)

synchronizing the account collaboration agent server counter clock with the at least first and second time clocks associated with the at least two web servers; (Moran, column 37, lines 41-61)

defining the database schema; (Cohen, column 5, lines 7-30)

securely logging into the at least first target web application; securely logging onto the at least second target web application after first logging into the first target web application (Cohen, column 4, lines 35-60.)

20. As per claim 14, Cohen-Moran-Belapurkar teaches the system further wherein the step of securely logging into the second target application further comprises executing the account collaboration agent server program upon sending a log-on request from the at least first web server to the at least second web server; (Cohen, column 4, lines 35-60)

extracting the user identification and associated first timestamp from the at least first web server session variable index at the same time the sent log-on request to the second web server is sent; storing the extracted first web server variables within the second web database; comparing the received extracted user identification variable sent from the first web server with the user identification variable stored in the second web server session variable index; denying access to the second web server if the received extracted user identification does not match the stored second web server user identification variable; clearing the first web server time stamp from the first web server session variable index; comparing the extracted first web server timestamp with a time indicated on the second server time clock; denying access to the second web application if the extracted timestamp and the indicated time on the second server time clock is greater than n seconds; allowing access to the second web application if the extracted timestamp and the indicated time on the second server time clock is equal to

or less than n seconds; and clearing extracted first web time stamp variable stored within the second web database (Belapurkar, paragraph 0028.)

21. As per claim 15, Cohen-Moran-Belapurkar teaches the system further wherein n equals three seconds (Belapurkar, paragraph 0028, specifically the use of window time differences.)

22. As per claim 16, Cohen-Moran-Belapurkar teaches the system further wherein the step of securely logging into the first target application further comprises: executing the account collaboration agent server program upon sending a log-on request from the at least second web server to the at least first web server; (Cohen, column 4, lines 35-60)

extracting the user identification and associated second timestamp from the at least second web server session variable index at the same time the sent log-on request to the first web server is sent; storing the extracted second web server variables within the first web database; comparing the received extracted user identification variable sent from the second web server with the user identification variable stored in the first web server session variable index; denying access to the first web server if the received extracted user identification does not match the stored first web server user identification variable; clearing the second web server time stamp from the second web server session variable index; comparing the extracted second web server timestamp with a time indicated on the first server time clock; denying access to the first web

application if the extracted timestamp and the indicated time on the first server time clock is greater than n seconds; allowing access to the first web application if the extracted timestamp and the indicated time on the first server time clock is equal to or less than n seconds; and clearing extracted second web time stamp variable stored within the first web database (Belapurkar, paragraph 0028.)

23. As per claim 17, Cohen-Moran-Belapurkar teaches the system further wherein n equals three seconds (Belapurkar, paragraph 0028, specifically the use of window time differences.)

Conclusion

24. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. This includes US PGPubs 2002/0156905 and 2002/0007460, and US Patent 6,243,816.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicholas Taylor whose telephone number is (571) 272-3889. The examiner can normally be reached on Monday-Friday, 8:00am to 5:30pm, with alternating Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is (703) 305-3718.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nicholas Taylor
Examiner
Art Unit 2141

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER